PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-319933

(43)Date of publication of application : 31.10.2002

(51)Int.Cl. H04L 9/08
H04L 12/18
// H04N 7/167

(21)Application number : 2001-122537

(22)Date of filing : 20.04.2001

(71)Applicant : SONY CORP

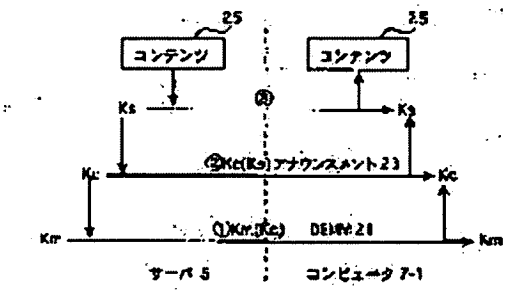
(72)Inventor : TOMINAGA HIROHISA
FUJII NOBORU
TAKEDA TAKASHI
TAKANO AKIYUKI

(54) COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a communication system, with which contents can be efficiently and safely transmitted from a server side to only a specified client.

SOLUTION: A server 5 and a computer 7-1 hold a master key Km. The server 5 encrypts a channel key Lc by the master key Km, places it on a DEMM 21, encrypts a contents key Ks by the channel key Kc, places it on an announcement 23, encrypts and sends contents 25 by the contents key Ks. The computer 7-1 decrypts the DEMM 21 by the master key Km, acquires the channel key Kc, decrypts the announcement 23 by the channel key Kc, acquires the contents key Ks and decrypts the contents 25 by the contents key Ks.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of

rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－319933
（Ｐ２００２－３１９９３３Ａ）
(43)公開日　平成14年10月31日(2002.10.31)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ			テーマコード（参考）
H04L 9/08		H04L 12/18			5C064
12/18		9/00	601	B	5J104
// H04N 7/167			601	E	5K030
		H04N 7/167		Z	

審査請求　未請求　請求項の数22　ＯＬ　（全８頁）

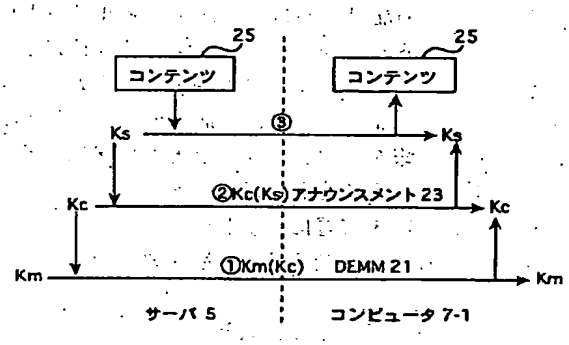
(21)出願番号　特願2001－122537(Ｐ2001－122537)
(22)出願日　平成13年４月20日(2001.4.20)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　冨長　裕久
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　藤井　昇
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101557
弁理士　萩原　康司

最終頁に続く

(54)【発明の名称】通信システム

(57)【要約】
【課題】　サーバ側から特定のクライアントにのみコンテンツを効率的に、かつ安全に送信できる通信システムを提供すること。
【解決手段】　サーバ５とコンピュータ７－１は、マスター鍵Ｋｍを保有している。サーバ５は、チャネル鍵Ｋｃをマスター鍵Ｋｍで暗号化し、ＤＥＭＭ２１に載せ、コンテンツ鍵Ｋｓをチャネル鍵Ｋｃで暗号化し、アナウンスメント２３に載せて、コンテンツ２５をコンテンツ鍵Ｋｓで暗号化して送る。コンピュータ７－１はマスター鍵ＫｍでＤＥＭＭ２１を解読し、チャネル鍵Ｋｃを取得し、チャネル鍵Ｋｃでアナウンスメント２３を復号化し、コンテンツ鍵Ｋｓを取得し、コンテンツ鍵Ｋｓでコンテンツ２５を復号化する。



1

【特許請求の範囲】

【請求項１】　サーバと端末装置とがネットワークで接続され、マルチキャスト方式で、前記サーバから前記端末装置へコンテンツを配信する通信システムであって、
前記サーバは、前記コンテンツ、チャネル情報及びクライアント情報を夫々暗号化して、鍵とともに前記端末装置に送り、
前記端末装置は、前記コンテンツ、前記チャネル情報、及び前記クライアント情報を所定の順序で前記鍵を用いて復号化することを特徴とする通信システム。

【請求項２】　前記クライアント情報は、制御情報ＤＥＭＭであり、前記チャネル情報はアナウンスメントであることを特徴とする請求項１記載の通信システム。

【請求項３】　前記サーバと前記端末装置は、マスター鍵を有しており、
前記サーバは、前記マスター鍵でチャネル鍵を暗号化し、暗号化されたチャネル鍵をクライアント情報に載せ、前記チャネル鍵でコンテンツ鍵を暗号化し、暗号化されたコンテンツ鍵をチャネル情報に載せ、前記コンテンツ鍵でコンテンツを暗号化し、前記端末装置に送り、
前記端末装置は、前記マスター鍵により前記クライアント情報を復号化してチャネル鍵を得て、このチャネル鍵で前記チャネル情報を復号化してコンテンツ鍵を得て、このコンテンツ鍵で、暗号化されたコンテンツを復号化することを特徴とする請求項１記載の通信システム。

【請求項４】　前記サーバは、前記チャネル情報と前記クライアント情報を、コンテンツを送信する通信帯域内で送信することを特徴とする請求項１記載の通信システム。

【請求項５】　前記サーバは、前記チャネル情報と前記クライアント情報をコンテンツを送信する前に送信することを特徴とする請求項４記載の通信システム。

【請求項６】　前記サーバは、前記チャネル情報と前記クライアント情報を、コンテンツとともに送信することを特徴とする請求項４記載の通信システム。

【請求項７】　端末装置にネットワークで接続され、マルチキャスト方式で、前記端末装置へコンテンツを配信するサーバであって、
前記コンテンツ、チャネル情報及びクライアント情報を夫々暗号化して、鍵とともに前記端末装置に送ることを特徴とするサーバ。

【請求項８】　前記クライアント情報は、制御情報ＤＥＭＭであり、前記チャネル情報はアナウンスメントであることを特徴とする請求項７記載のサーバ。

【請求項９】　マスター鍵を有しており、前記マスター鍵でチャネル鍵を暗号化し、暗号化されたチャネル鍵をクライアント情報に載せ、前記チャネル鍵でコンテンツ鍵を暗号化し、暗号化されたコンテンツ鍵をチャネル情報に載せ、前記コンテンツ鍵でコンテンツを暗号化し、前記端末装置に送ることを特徴とする請求項７記載のサーバ。

2

【請求項１０】　前記チャネル情報と前記クライアント情報を、コンテンツを送信する通信帯域内で送信することを特徴とする請求項７記載のサーバ。

【請求項１１】　前記チャネル情報と前記クライアント情報をコンテンツを送信する前に送信することを特徴とする請求項１０記載のサーバ。

【請求項１２】　前記チャネル情報と前記クライアント情報を、コンテンツとともに送信することを特徴とする請求項１０記載のサーバ。

【請求項１３】　サーバとネットワークで接続され、マルチキャスト方式で、前記サーバから配信されるコンテンツを受信する端末装置であって、
前記サーバは、前記コンテンツ、チャネル情報及びクライアント情報を夫々暗号化して、鍵とともに前記端末装置に送り、
前記コンテンツ、前記チャネル情報、及び前記クライアント情報を所定の順序で前記鍵を用いて復号化することを特徴とする端末装置。

【請求項１４】　前記クライアント情報は、制御情報ＤＥＭＭであり、前記チャネル情報はアナウンスメントであることを特徴とする請求項１３記載の端末装置。

【請求項１５】　前記サーバと前記端末装置は、マスター鍵を有しており、
前記サーバは、前記マスター鍵でチャネル鍵を暗号化し、暗号化されたチャネル鍵をクライアント情報に載せ、前記チャネル鍵でコンテンツ鍵を暗号化し、暗号化されたコンテンツ鍵をチャネル情報に載せ、前記コンテンツ鍵でコンテンツを暗号化し、前記端末装置に送り、
前記マスター鍵により前記クライアント情報を復号化してチャネル鍵を得て、このチャネル鍵で前記チャネル情報を復号化してコンテンツ鍵を得て、このコンテンツ鍵で、暗号化されたコンテンツを復号化することを特徴とする請求項１３記載の端末装置。

【請求項１６】　前記チャネル情報と前記クライアント情報をコンテンツを送信する通信帯域内で受信することを特徴とする請求項１３記載の端末装置。

【請求項１７】　前記チャネル情報と前記クライアント情報をコンテンツを送信する前に受信することを特徴とする請求項１６記載の端末装置。

【請求項１８】　前記チャネル情報と前記クライアント情報を、コンテンツとともに受信することを特徴とする請求項１６記載の端末装置。

【請求項１９】　請求項７から請求項１２までのいずれかに記載されたサーバとしてコンピュータを機能させるプログラム。

【請求項２０】　請求項７から請求項１２までのいずれかに記載されたサーバとしてコンピュータを機能させるプログラムを記録した記録媒体。

【請求項２１】　請求項１３から請求項１８までのいず

れかに記載された端末装置としてコンピュータを機能させるプログラム。

【請求項２２】　請求項１３から請求項１８までのいずれかに記載された端末装置としてコンピュータを機能させるプログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータネットワークや、人工衛星を用いたサテライトネットワーク等において、マルチキャスト方式で通信を行う通信システムに関するものである。

【０００２】

【従来の技術】昨今、サーバとクライアントコンピュータとが、インターネット等のコンピュータネットワークや人工衛星を用いたサテライトネットワーク等で接続され、放送と同様にサーバからクライアントにコンテンツ等の配信を行うシステムが実現されつつある。

【０００３】

【発明が解決しようとする課題】ところで、このような通信システムにおいて、限られたクライアントにのみサーバ側からコンテンツを効率的に、かつ安全に送信したいという要望がある。

【０００４】本発明はこのような問題に鑑みてなされたもので、その目的とするところは、サーバ側から特定のクライアントにのみコンテンツを効率的に、かつ安全に送信できる通信システムを提供することにある。

【０００５】

【課題を解決するための手段】前述した目的を達成するために本発明は、サーバと端末装置とがネットワークで接続され、マルチキャスト方式で、前記サーバから前記端末装置へコンテンツを配信する通信システムであって、前記サーバは、前記コンテンツ、チャネル情報及びクライアント情報を夫々暗号化して、鍵とともに前記端末装置に送り、前記端末装置は、前記コンテンツ、前記チャネル情報、及び前記クライアント情報を所定の順序で前記鍵を用いて復号化することを特徴とする通信システムである。

【０００６】ここで、サーバとは、コンテンツを配信する機能等を有するコンピュータである。端末装置とは、各家庭等に設置されるようなパーソナルコンピュータ、携帯型端末装置等である。ネットワークとは、通信回路網であり、有線、無線を問わない。ネットワークとしては、例えばインターネット等があり、人工衛星を介したサテライトネットワークも含まれる。

【０００７】マルチキャスト方式とは、端末装置がマルチキャストアドレスを獲得し、このマルチキャストアドレスによってサーバにアクセスし、コンテンツの配信を受ける方式である。このような、マルチキャスト方式では限られた端末装置がコンテンツを受信することができる。コンテンツとは、画像情報や音楽情報等である。クライアント情報とは、制御情報（ＤＥＭＭ）と称され、コンテンツの配信の対象となるクライアントのＩＤ等の情報である。

【０００８】チャネル情報は、アナウンスメントと称され、コンテンツに関する情報である。本発明では、サーバは、コンテンツ、チャネル情報及びクライアント情報を夫々暗号化して、鍵とともに端末装置に送り、端末装置は、コンテンツ、チャネル情報、及びクライアント情報を鍵を用いて所定の順序で復号化する。

【０００９】即ち、前記サーバと前記端末装置は、マスター鍵を有しており、前記サーバは、前記マスター鍵でチャネル鍵を暗号化し、暗号化されたチャネル鍵をクライアント情報に載せ、前記チャネル鍵でコンテンツ鍵を暗号化し、暗号化されたコンテンツ鍵をチャネル情報に載せ、前記コンテンツ鍵でコンテンツを暗号化し、前記端末装置に送り、前記端末装置は、前記マスター鍵により前記クライアント情報を復号化してチャネル鍵を得て、このチャネル鍵で前記チャネル情報を復号化してコンテンツ鍵を得て、このコンテンツ鍵で、暗号化されたコンテンツを復号化する。

【００１０】マスター鍵は、チャネル鍵を暗号化および復号化する鍵であり、チャネル鍵は、コンテンツ鍵を暗号化及び復号化する鍵である。コンテンツ鍵は、コンテンツを暗号化及び復号化する鍵である。本発明では、サーバは、前記チャネル情報と前記クライアント情報とコンテンツを送信する通信帯域内で送信したり、前記チャネル情報と前記クライアント情報をコンテンツを送信する前に送信したり、前記チャネル情報と前記クライアント情報を、コンテンツとともに送信する。

【００１１】また、本発明は、端末装置にネットワークで接続され、マルチキャスト方式で、前記端末装置へコンテンツを配信するサーバであって、前記コンテンツ、チャネル情報及びクライアント情報を夫々暗号化して、鍵とともに前記端末装置に送ることを特徴とするサーバである。

【００１２】即ち、このサーバは、マスター鍵を有しており、前記マスター鍵でチャネル鍵を暗号化し暗号化されたチャネル鍵をクライアント情報に載せ、前記チャネル鍵でコンテンツ鍵を暗号化し、暗号化されたコンテンツ鍵をチャネル情報に載せ、前記コンテンツ鍵でコンテンツを暗号化し、前記端末装置に送る。

【００１３】また、本発明は、サーバとネットワークで接続され、マルチキャスト方式で、前記サーバから配信されるコンテンツを受信する端末装置であって、前記サーバは、前記コンテンツ、チャネル情報及びクライアント情報を夫々暗号化して、鍵とともに前記端末装置に送り、前記コンテンツ、前記チャネル情報、及び前記クライアント情報を所定の順序で前記鍵を用いて復号化することを特徴とする端末装置である。

【００１４】即ち、この端末装置は、マスター鍵を有し

ており、前記マスター鍵によりサーバから送られるクライアント情報を復号化してチャネル鍵を得て、このチャネル鍵でチャネル情報を復号化してコンテンツ鍵を得て、このコンテンツ鍵で、暗号化されたコンテンツを復号化する。更に、前述したサーバや端末装置としてコンピュータを機能させるプログラムや、このプログラムを記録したＣＤ－ＲＯＭ等の記録媒体も本発明に含まれる。

【００１５】

【発明の実施の形態】以下、図面に基づいて本発明の実施の形態を詳細に説明する。図１は、本発明の実施の形態に係る通信システム１の概略構成図である。この通信システム１はインターネット等のネットワーク３にサーバ５、クライアント側の端末機としてのコンピュータ７－１、７－２、７－３……等が接続されて構成される。

【００１６】ネットワーク３は、インターネット等のネットワークであり、有線、無線を含む。尚、ネットワーク３には、人工衛星を介してコンテンツの配信を行うサテライトネットワークも含まれる。サーバ５は、コンテンツの配信等を行う。コンピュータ７－１、７－２……は、例えば一般ユーザの所有するコンピュータである。このコンピュータに代えて携帯型端末機や、電話機能を有する端末機（携帯電話）を用いてもよい。

【００１７】次に、この通信システム１の動作について説明する。図２は、サーバ５からコンピュータ７側にコンテンツを配信する場合の説明図である。図２に示すように、サーバ５からコンピュータ７－１等にコンテンツを配信する場合、コンテンツ２５の配信と同時に伝送制御情報としてＤＥＭＭ２１とアナウンスメント２３を送信する。例えば、午後１時から午後３時の間にコンテンツ２５が配信され、このコンテンツ２５の配信と同時にＤＥＭＭ２１とアナウンスメント２３が配信される。このように、ＤＥＭＭ２１とアナウンスメント２３は、コンテンツ２５を送信する通信帯域内で送信される。

【００１８】ＤＥＭＭ（Ｄａｔａ　Ｅｎｔｉｔｌｅｍｅｎｔ　Ｍａｎａｇｅｍｅｎｔ　Ｍｅｓｓａｇｅ）は、クライアント情報である。図３は、ＤＥＭＭ２１に搭載される情報を示すもので、ＤＥＭＭ２１は、ＤＥＭＭが暗号化されているかどうかと暗号化の種類を示すフラグ３１、クライアントＩＤ３３、受信許可が与えられているチャネルＩＤ３５、コンテンツ鍵Ｋｓが含まれているチャネル鍵（アナウンスメントの復号鍵）Ｋｃ３７等を有する。

【００１９】ＤＥＭＭが暗号化されているかどうかと、暗号化の種類を示すフラグ３１は、例えばＤＥＭＭ２１が暗号化されているのであれば「１」であり、更に「ＤＥＳ」で暗号化されていれば暗号化の種類を示すフラグ「２」が付加される。クライアントＩＤ３３は、コンテンツを受信することができるクライアント側のコンピュータ７－１等のＩＤ番号である。

【００２０】受信許可が与えられているチャネルＩＤ３５は、クライアントＩＤ３３で示されるクライアントが受信できるチャネルを示すもので、例えばコンピュータ７－１に与えられるチャネルのＩＤ番号である。コンテンツ鍵Ｋｓが含まれているチャネル鍵Ｋｃ３７は、クライアント側がアナウンスメント２３を解読するための復号鍵である。

【００２１】図４は、アナウンスメント２３に搭載される情報を示す。アナウンスメント２３は、アナウンスメントが暗号化されているかどうかと、暗号化の種類を示すフラグ４１、チャネルを識別する番号（チャネルＩＤ）４３、コンテンツを識別する番号（コンテンツＩＤ）４５、コンテンツが配信されるマルチキャストアドレス４７、マルチキャストのポート番号４９、コンテンツ鍵Ｋｓ５１等を有する。

【００２２】アナウンスメントが暗号化されているかどうかと、暗号化の種類を示すフラグ４１は、例えばアナウンスメントが暗号化されている場合には「１」であり、更に「ＤＥＳ」で暗号化されていれば暗号化の種類を示す「２」が付加される。

【００２３】チャネルＩＤ４３は、クライアントが利用できるチャネルを示す。コンテンツＩＤ４５は、コンテンツ鍵Ｋｓ５１で復号化されるコンテンツ２５のＩＤ番号である。マルチキャストアドレス４７、マルチキャストのポート番号４９は、コンテンツ２５が配信されるマルチキャストアドレス及びポート番号である。

【００２４】図５、図６は、この通信システム１の処理を示すフローチャートであり、図７は、この通信システム１における鍵情報の伝送手順を示す図、図８はクライアント側の処理を示す図である。以下の例では、クライアントとしてコンピュータ７－１を取り上げて説明する。

【００２５】図５に示すように、サーバ５とクライアント側のコンピュータ７－１は、予めマスター鍵Ｋｍを有している（ステップ５０１、５０２）。このマスター鍵Ｋｍは、サーバ５及びクライアント側のコンピュータ７－１等にＣＤ－ＲＯＭ等で送付しておく。または、ネットワーク３を用いて、サーバ５とコンピュータ７－１が、ある共通の数字からマスター鍵Ｋｍを生成するアルゴリズムを保有し、双方でマスター鍵を生成するようにしてもよい。

【００２６】サーバ５は、制御情報ＤＥＭＭ２１をマスター鍵Ｋｍで暗号化する（ステップ５０３）。即ち図３に示す制御情報ＤＥＭＭ２１が暗号化され、チャネル鍵Ｋｃもマスター鍵Ｋｍで暗号化され、チャネル鍵Ｋｃ３７としてＤＥＭＭ２１に搭載される。サーバ５は、所定のチャネルのアナウンスメント２３をチャネル鍵Ｋｃで暗号化する（ステップ５０４）。即ち、図４に示すアナウンスメント２３が暗号化され、コンテンツ鍵Ｋｓ５１もチャネル鍵Ｋｃで暗号化される。

【００２７】更にサーバ５は、コンテンツ２５をコンテンツ鍵Ｋｓで暗号化する(ステップ５０５)。そして、図２に示すように、コンテンツ２５をＤＥＭＭ２１、アナウンスメント２３とともに送信する(ステップ５０６)。コンピュータ７－１は、予め保有しているマスター鍵Ｋｍにより、制御情報ＤＥＭＭ２１を復号化する(ステップ５０７)。即ち、図３に示す制御情報ＤＥＭＭ２１が復号化され、チャネルを特定するＩＤと、そのチャネルのチャネル鍵Ｋｃ３７を取得する(ステップ５０８)。

【００２８】チャネルを特定するＩＤ６１は、システム固有のＩＤ番号、サーバ５のＩＤ番号、チャネルＩＤ番号３５等を有する。ＤＥＭＭ２１に搭載された情報は次のＤＥＭＭ２１がくるまで、コンピュータ７－１に保存されるが、次のＤＥＭＭ２１を受信した時点ですべて更新する。

【００２９】このため、内容が空のＤＥＭＭ２１を受信した場合、クライアントが受信できるコンテンツをなくすことができる。このように、サーバ５がＤＥＭＭ２１の設定を変更すれば、その設定の変更が直ちにクライアント（コンピュータ７－１等）に反映される。

【００３０】コンピュータ７－１は、当該チャネルのアナウンスメント２３をチャネル鍵Ｋｃで解読し、コンテンツ鍵Ｋｓ５１を取得し、チャネル情報６３を得る(ステップ５０９)。チャネル情報６３は、チャネルＩＤ４３やマルチキャストアドレス４７、ポート番号４９等である。そして、コンピュータ７－１は、取得されたコンテンツ鍵Ｋｓを用いてコンテンツ２５を復号化し、解読する。

【００３１】図８は、コンピュータ７－１側の処理を示す説明図である。コンピュータ７－１は、マスター鍵Ｋｍを保有しており、ＤＥＭＭ２１をマスター鍵Ｋｍで復号化し、第１チャネル鍵Ｋｃ１、第１チャネルを特定するＩＤ６１－１、第２チャネル鍵Ｋｃ２、第２チャネルを特定するＩＤ６１－２等を得る。

【００３２】コンピュータ７－１は、アナウンスメント２３－１を第１チャネル鍵Ｋｃ１で復号化し、チャネル情報６３－１、コンテンツ鍵Ｋｓ１を得る。また、コンピュータ７－１は、アナウンスメント２３－２を第２チャネル鍵Ｋｃ２で復号化し、チャネル情報６３－２、コンテンツ鍵Ｋｓ２を得る。このように、アナウンスメント２３－１、２３－２は、チャネルに対応したものである。

【００３３】そして、コンピュータ７－１は、コンテンツ２５－１をコンテンツ鍵Ｋｓ１で復号化し、コンテンツ２５－２をコンテンツ鍵Ｋｓ２で復号化する。

【００３４】このように、本実施の形態によれば、サーバ５は、アナウンスメント２３を暗号化することで、チャネル単位でクライアントのアクセスをコントロールすることができる。また、限られた時間と周波数帯域の中で、ＤＥＭＭ２１、アナウンスメント２３およびコンテンツ２５を送信することができる。

【００３５】そして、コンテンツ２５に関する情報をアナウンスメント２３に搭載し、クライアントに関する情報をＤＥＭＭ２１に搭載して、ＤＥＭＭ２１とアナウンスメント２３とを分離して送信するので、全体の制御データ量を減らすことができる。更に、コンテンツ鍵Ｋｓ、チャネル鍵Ｋｃ、マスター鍵Ｋｍという三つの鍵を用いて、コンテンツを解読するようにしたので、コンテンツを特定のクライアントにのみ安全に配信することができる。

【００３６】更に、コンテンツ鍵Ｋｓをコンテンツごとに変化させた場合でも、アナウンスメント２３に含まれる情報を書き換えるだけでクライアント側のコンピュータ７はコンテンツ２５の受信が行え、毎回コンテンツ２５を送信するごとにマスター鍵Ｋｍを用いて、個別にデータ送信をする必要がないので、コンテンツ２５の限定配信を効率的に行うことができる。

【００３７】図９、図１０は、伝送制御情報の別の送信方式を示すもので、図９では、ＤＥＭＭ２１、アナウンスメント２３をサーバ５からクライアント側のコンピュータ７に送信した後、コンテンツ２５を送信する。ＤＥＭＭ２１、アナウンスメント２３は、コンテンツの周波数帯域と同じ周波数帯域を用いる。

【００３８】図１０では、ＤＥＭＭ２１、アナウンスメント２３を送信した後、コンテンツ２５とともにＤＥＭＭ２１、アナウンスメント２３を送信する。図９、図１０に示す場合は、コンテンツ２５の送信開始と同時にすべてのクライアントに受信を開始させることが可能である。

【００３９】また、図２、図１０の場合、常にクライアントの受信状態を変化させることができる。尚、図２、図１０の方式では、コンテンツ２５の帯域を圧迫しすぎないように、ＤＥＭＭ２１やアナウンスメント２３のビットレートの上限値を以下のように定める。

【００４０】まず、数値で例えば、１００Ｋｂｐｓのように上限を定める。次に、全体の帯域に対する上限比率を例えば、５％に定める。そして、ＤＥＭＭ２１やアナウンスメント２３の伝送制御データの送信は、この二つの上限値を超えないようにする。このように上限値を定めることにより、オーバースペックを防ぐことができる。

【００４１】

【発明の効果】以上、詳細に説明したように本発明によれば、サーバ側から特定のクライアントにのみコンテンツを効率的に、かつ安全に送信できる通信システムを提供することができる。

【図面の簡単な説明】

【図１】　通信システム１の概略構成図

【図２】　アナウンスメント２１とコンテンツ２３の送信の説明図

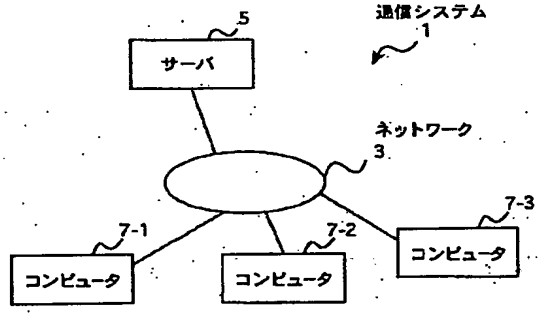
9

【図３】　ＤＥＭＭ２１に搭載される情報を示す図
【図４】　アナウンスメント２３に搭載される情報を示す図
【図５】　通信システム１の概略動作を示すフローチャート
【図６】　通信システム１の概略動作を示すフローチャート
【図７】　通信システム１における鍵の伝送手順を示す図
【図８】　クライアント側のコンピュータ７による復号化を示す図
【図９】　アナウンスメント２１とコンテンツ２３の送信の説明図

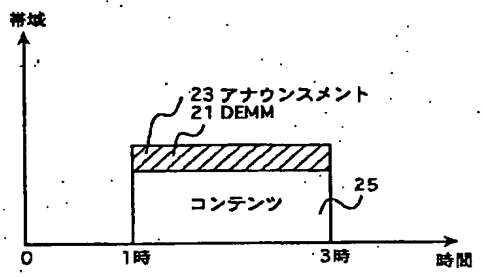
10

【図１０】　アナウンスメント２１とコンテンツ２３の送信の説明図
【符号の説明】
1 ……通信システム
3 ……ネットワーク
5 ……サーバ
7 ……コンピュータ
２１……ＤＥＭＭ
２３……アナウンスメント
２５……コンテンツ

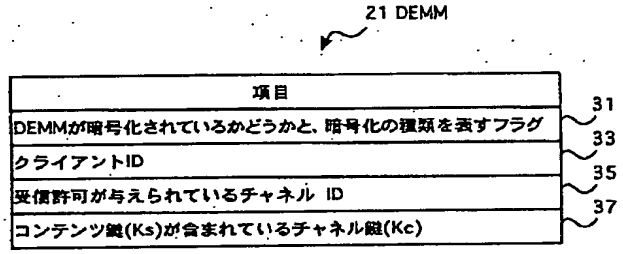
【図１】



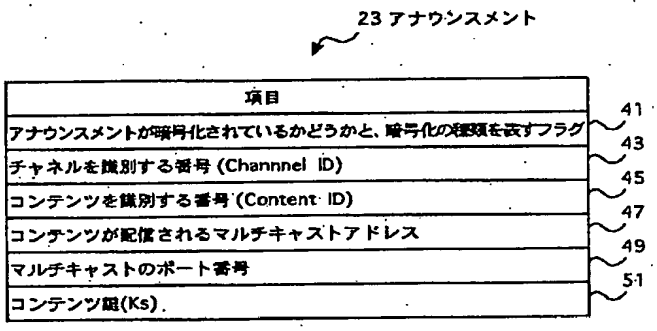
【図２】



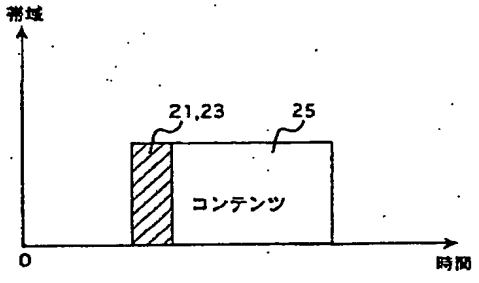
【図３】



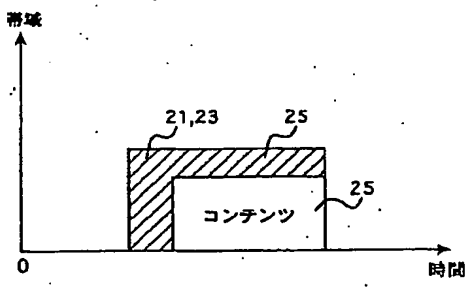
【図４】



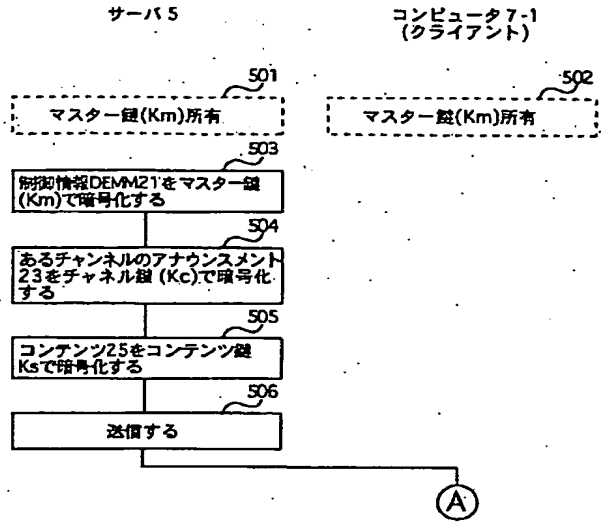
【図９】



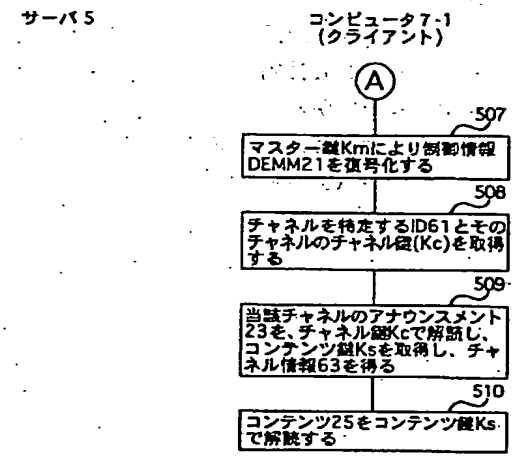
【図１０】



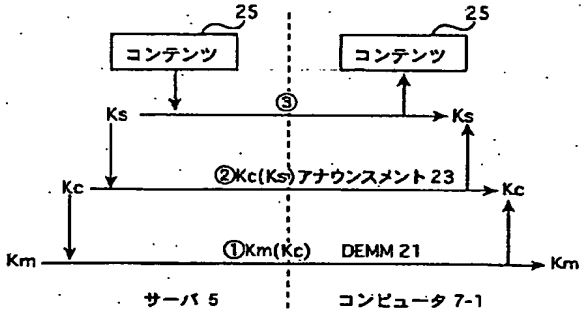
【図５】


サーバ５
コンピュータ７-１
(クライアント)
501
マスター鍵(Km)所有
502
マスター鍵(Km)所有
503
制御情報DEMM21をマスター鍵(Km)で暗号化する
504
あるチャンネルのアナウンスメント23をチャネル鍵(Kc)で暗号化する
505
コンテンツ25をコンテンツ鍵Ksで暗号化する
506
送信する
A

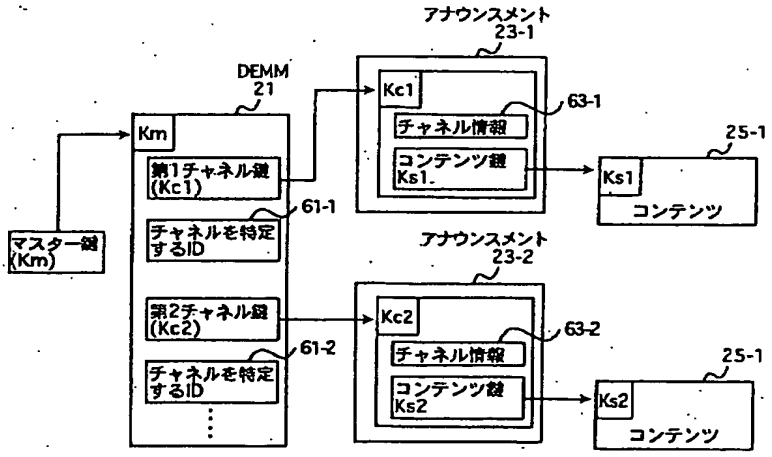
【図６】


サーバ５
コンピュータ７-１
(クライアント)
A
507
マスター鍵Kmにより制御情報DEMM21を復号化する
508
チャネルを特定するID61とそのチャネルのチャネル鍵(Kc)を取得する
509
当該チャネルのアナウンスメント23を、チャネル鍵Kcで解読し、コンテンツ鍵Ksを取得し、チャネル情報63を得る
510
コンテンツ25をコンテンツ鍵Ksで解読する

【図７】


25
コンテンツ
25
コンテンツ
③
Ks
Ks
②Kc(Ks)アナウンスメント23
Kc
Kc
①Km(Kc)　DEMM 21
Km
Km
サーバ５
コンピュータ７-１

【図８】


アナウンスメント
23-1
DEMM
21
Km
第1チャネル鍵
(Kc1)
61-1
チャネルを特定するID
第2チャネル鍵
(Kc2)
61-2
チャネルを特定するID
マスター鍵
(Km)
Kc1
チャネル情報
63-1
コンテンツ鍵
Ks1
25-1
Ks1
コンテンツ
アナウンスメント
23-2
Kc2
チャネル情報
63-2
コンテンツ鍵
Ks2
25-1
Ks2
コンテンツ

フロントページの続き

(72) 発明者　武田　貴志
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72) 発明者　高野　明幸
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5C064 AA06 AD14 BA07 BB02 BC17 BC22 BD08 BD14 CA14 CA16 CB01 CC01 CC04
5J104 AA16 EA07 EA18 NA02 PA07
5K030 GA15 HB19 KA01 KA02 LD02 LD07